Machine Learning Models:

Bust Out Fraud Detection

Vertical

- **Industry:** Financial Services, Banking
- **Industry Detail:** Consumer Credit Card
- **Function:** Credit Card Issuer

Use Case Highlights

- Avoid credit loss by detecting those users who intend to rack up charges on a credit card but never pay.
- Collection of models using transactional history, payments, and non-monetary activity to detect and prevent fraud before it happens.
- Get more lead-time to take pre-emptive action by identifying bust-out customers before they occur with additional data sources, advanced modeling techniques, and decades of combined fraud experience.

Use Case

- A bust-out is a type of credit card fraud where an individual applies for a credit card, establishes a normal usage pattern and solid repayment history, then racks up numerous charges and maxes out the card with no intention of paying the bill.
- The objective is to identify fraudsters early on before they rack up credit card charges.

Technical Highlights

- A non-linear adaptive analytics approach used for credit abuse detection to provide a better predictive power and ability to identify accounts earlier in the cycle.
- Dynamic Bust-out Pattern Analysis identifies interconnected patterns between transaction types and velocity, high risk purchases and non-monetary information.
  - Rapid: Quickly increase spend and make large payments to free up more opportunity to buy.
  - Collusive Merchants: Large purchases made at single (often newer) merchants.
  - Long Play: Spending and payments increase over many months. Customer continues to spend up to their full credit limit and then payments bounce.
- Neural Network Model for Bust-out Prediction significantly improves detection accuracy, 5 days earlier.
  - Neural Networks uncover the hidden non-linear relationships between inputs and outcomes to predict small probability events.
  - Customer activity patterns are monitored on a daily basis to identify predictive patterns.

Ready to get started?

To learn more, please contact our experts at info@electrifai.net

10 Exchange Place, 11th Floor, Jersey City, NJ 07302
www.electrifai.net

ElectrifAi

Machine Learning Models:

Bust Out Fraud Detection

Business Impact

- $60MM annual savings
- 5 to 7-day earlier identification
- No rise in false positives
- Completely integrated into customer's environment

Data Sources and Features

- Efficiency of bust-out fraud detection increased by utilizing more data inputs and sophisticated neural network models to find more fraud.
- Developed an "After the Fact" model to accurately assess the real bust-out baseline, built predictive model using the expanded baseline, and finally estimated savings under various scenarios of analyst capacity.
- Transaction data examined to create variables based on high risk merchandise to capture more granular risk behaviors.

Leveraging Model Output

Data In

- Early intervention
- Card transactions
- Customer service interactions
- Underwriting
- Transfer information
- Payment information
- Customer demographics

Data Out

- See compromise window, pre-fraud distribution
- Probability score for Bust-out Fraud at account level
- Score distribution over time
- Card burn rate trends
- Card fraud usage distributions

Ready to get started?

To learn more, please contact our experts at info@electrifai.net

10 Exchange Place, 11th Floor, Jersey City, NJ 07302
www.electrifai.net

ElectrifAi